address translation devices constantly reuse the mappings used for network address translation even when a certain fraction of the packets communicated between the first computer device and the second computer device are lost in the network.

REMARKS

The abstract has been cancelled from page 1 of the specification and a substitute abstract on a separate page numbered as page 56 is submitted herewith.

With regard to the listing of references, these references are prior art, but they have been incorporated by reference into the specification. None of them are believed to be material to the claimed invention as they just teach the prior art protocols that are well known and some of which are used as building blocks for the invention. Since they are properly incorporated by reference in the specification properly, a separate Information Disclosure Statement listing them all and providing copies is not believed to be necessary.

With regard to the anticipation rejection, the Examiner is respectfully request to withdraw this rejection for the reason that not all elements of the claims at bar are found in the Nessett patent, 6,055,236. Specifically, the claims at bar recite encapsulating packets conforming to a first protocol into packets conforming to a second protocol which is capable of traversing network address translation. While Nessett does teach encapsulation of packets into other packets, the network address translations Nessett teaches these packets as traversing is not the same network address translation recited in the claims at bar. Specifically, Nessett teaches a new type of network address translation called distributed network address translation which relies upon a protocol called PAP which is absent from the prior art network address translation processes recited in the claims at bar. The original claims at bar are designed to provide a method to provide a way for packets conforming to a protocol such as IPsec which have not been able to traverse network address translation processes to be encapsulated in another packet type which can successfully traverse prior art network address translations. Specifically, in the preferred class of embodiments, IPsec packets are encapsulated into UDP or TCP packets which can be successfully transmitted across NAT, and then the IPsec packets are recovered at the destination.

We turn now to developing more fully and providing citations to evidentiary support for the argument summarized above. As evidence that the application at bar is speaking of prior art network address translations which would not understand the PAP protocol of Nessett, consider the following passage from the specification beginning at page 5, line 20:

> Fig. 1c illustrates an exemplary practical network communication situation where a transmitting node 181 is located in a first local area network (also known as the first private network) 182, which has a port NAT 183 to connect it to a wide-area general packet-switched network 184 like the Internet. The latter consists of a very large number of nodes interconnected in an arbitrary way. A receiving node 185 is located in a second local area network 186 which is again coupled to the wide-area network through a NAT 187....
>
> The purpose of Fig. 1c is to emphasize the fact that the communicating nodes are aware of neither the number or nature of the intermediate devices through which they communicate nor the nature of transformations that take place. In addition to NATs, there are other types of devices on the Internet that may legally modify packets as they are transmitted. A typical example is a protocol converter, whose main job is to convert the packet to a different protocol without disturbing normal operation. Using them leads to problems very similar to the NAT case. A fairly simple but important example is converting between IPv4 and IPv6, which are different versions of the Internet Protocol. Such converters will be extremely important and commonplace in the near future. A packet may undergo several conversions of this type during its travel, and it is possible that the endpoints of the communication actually use a different protocol. Like NAT, protocol conversion is often performed in routers and firewalls.
>
> It is well known in the IPSEC community that the IPSEC protocol does not work well across network address translations. The problem has been discussed at least in the references given as HoldregeSrisuresh99 and Rekhter99.

The underlined portion emphasizes the point we wish to make in this argument.

That point is that the transmitting and receiving nodes in the networks in which the invention is applied are not aware of the presence of NAT devices between them on the network nor the type of processing translations that goes on in them. Further, the NAT translators in the networks in which the claimed invention operates are not capable of processing IPsec packets therethrough without altering them in a way that disables the IPsec protocol. This is what creates the problem the invention solves.

The problem the invention solves is how to transmit IPsec packets across NAT or protocol conversions that do not understand IPsec packets. The invention solves this problem by encapsulating the IPsec packets into packets having a protocol the NAT translators and protocol converters do understand (TCP or UDP). This way, the IPsec packets can be encapsulated in UDP packets and sent through any number of NAT and protocol conversions regardless of where they occur, what exact processing goes on in each NAT or protocol conversion and regardless of the particular type of NAT involved. The transmitter of IPsec packets in a network using the invention does not need to be aware that a NAT translator exists or that it will do IP address translation work on the IPsec packets. The NAT translator does not have to have any special capabilities.

This is not the same invention as is taught in Nessett because in Nessett, the NAT translators need to have special capabilities and the transmitters and receivers have to know the DNAT translators are there and how to carry out a PAP protocol with the DNAT translators of Nessett's invention. The Nessett transmitters and receivers will not work with just any old NAT like the transmitters and receivers of the invention -- they will only work with the specially adapted DNAT translators using the PAP protocol taught in Nessett. Therefore, Nessett does not teach the same invention.

Evidence of the fact that the Nessett transmitters and receivers need to know about the presence of DNAT translators is found from the following passages from the

Nessett specification.

The following passage from Col. 25, Lines 54 (hereafter citations to column and line numbers will take the format Cxx/Lyy) shows that Nessett knows that prior art NAT routers screw up IPsec packets when they process them and thus Nessett recognizes the same problem addressed by the invention:

> As was discussed above, NAT routers known in the art need to modify IP 48 packets. However, once an IP 48 packet is protected by IPsec, it cannot be modified anywhere along its path to the IPsec destination. NAT routers known in the art typically violate IPsec by modifying packets. In addition, even if a NAT router did not need to modify the packets it forwards, it must be able to read the TCP 58 or UDP 60 port numbers. If ESP is used by a local endpoint, the port numbers will be encrypted, so the NAT router will not be able to complete its required mapping.
>
> Local network devices on a LAN that use NAT possess only local, non-unique IP 48 addresses. These do not comprise a security name space that is suitable for binding a public key to a unique identity (i.e., a unique global IP 48 address). Without this binding, it is typically not possible to provide the authentication necessary for establishment of SAs. Without authentication, neither endpoint can be certain of the identity of their counter part, and thus cannot establish a secure and trusted connection via a SA. However, DNAT described above, can be used with IPsec to overcome some of the problems with NAT devices known in the art.

The second paragraph in this passage indicates at the underlined portion that DNAT (the special NAT taught by Nessett) can be used to resolve the problems with IPsec created by the type of NAT translators which the invention of the claims at bar can handle.

The following passages from C26/L9 et seq. teach how Nessett solve the above identified problem:

> A network device using DNAT as described above may also desire to establish a secure virtual connection to an external network device using IPsec (e.g., SPIs). Such a network device would request and use locally unique ports and use DNAT as was described above. In addition, the network device may request locally unique security values to use DNAT with IPsec.
>
> FIG. 19 is a flow diagram illustrating a Method 274 for distributed network address translation with security. At Step 276, a first network device on a first computer network requests with a first protocol, one or more locally unique security values

> (e.g., SPIs) from a second network device on the first computer network and for distributed network address translation. The one or more locally unique security values are used to identify security associations for data reception on the first network device during secure communications with a third network device on a second external network. At Step 278, the one or more locally unique security values are received on the first network device from the second network device with the first protocol. The one or more locally unique security values are stored on the first network device at Step 280. The one or more locally unique security values can be used to identify a unique security association for secure communications and used for distributed network address translation. A unique security association identified by the first computer on the first network is used for reception of packets on the first computer.
>
> In one exemplary preferred embodiment of the present invention, the first network device is a network device (14, 16, 18, 20, 22, and 24), the second network device is the router 26, the first protocol is the PAP 64, the one or morelocally unique security values are SPIs used with IPsec, including AH or ESP. In one exemplary preferred embodiment of the present invention, the locally unique security values are obtained with the PAP 64 using a PAP 64 security request message 67, a PAP 64 security response message 69, and a PAP 64 security invalidate message 71.

The underlined portions of the next to last paragraph and last paragraph of this passage indicate that the transmitting node on the LAN connected to a router must know that the router is there and that it can understand the PAP protocol. Further, the transmitter also needs to know what the particular security messages are of the PAP protocol for implementing security and be able to send and receive them, and it must know that the router is an NAT translator which can understand these PAP security messages and respond appropriately with a locally unique security value (SPI). Obviously, not just any transmitting node will do and the tranmitting node must know the NAT exists and must know that it understands PAP security messages and must know how to send and receive PAP security messages.

This Nessett system is not the same method as described in the claims at bar when properly interpreted in accordance with the invention described in the specification. Properly interpreted, the claims generally call for determining what NATs occur between the transmitter and receiver, and then encapsulating packets of a

protocol that cannot traverse NAT (such as IPsec -- same teaching applicable to protocol conversions also) in packets of a protocol that can traverse NAT (or protocol conversions), transmitting these second protocol packets to the receiver and decapsulating them there to recover the packets of the original first protocol. No special NATs or protocol conversions are needed and the transmitter and receiver do not need to understand PAP or be able to send or receive PAP security messages.

The PAP protocol is unique and proprietary to 3Com and will not generally be found in any NAT translator not built by or licensed by 3COM. It is certainly not present in every NAT translator everywhere on the internet. This means that while the invention can operate anywhere with whatever NAT translators it happens to encounter, the Nessett transmitters and receivers can only send IPsec packets through NAT translators that understand the PAP protocol.

The PAP protocol is used to request locally unique port numbers or SPIs (depending upon the embodiment) from an NAT which understands PAP request messages and can send PAP response messages. Not all NATs can do this.

The PAP and DNAT processes disclosed in Nessett do not encapsulate IPsec packets in UDP or TCP packets. There is encapsulation that happens in DNAT, but it is not the same encapsulation as is used in the method of the invention. The encapsulation taught in the DNAT of Nessett is described at C15/L42-67 through C16/L2. In the DNAT method using PAP, a LAN is coupled by a router to an external WAN such as the internet. Every node and every process on a node on the LAN does not have a unique IP address. Instead, the entire LAN has a single unique IP address. To provide sufficient address resolution so that packets can be sent and received by individual processes on the LAN, the PAP protocol is used to communicate between each node and the router. The router must understand the PAP protocol. The PAP protocol is used to request locally unique

port designations that can be used in an Outer IP header. The process is described in Figure 10 of Nessett, and the first step involves a network device on the LAN sending a TCP request to a server out on the internet (such as server 39 on the internet in Figure 1. This TCP request includes the globally unique IP address of the server out on the internet. The TCP packet has as its source address the globally unique IP address of the entire LAN and has as a source port a locally unique port obtained from the router 26 in Figure 1 coupling the LAN to the internet. The locally unique port number is obtained using the PAP request message when the network device which is making the TCP request was booted. C10/L60. The unique port number for the network device making the TCP request replaces a default TCP port when the network device was booted and makes the PAP request. C15/L32. The TCP request is sent down the network device's protocol stack until it reaches the network devices network interface card. C15/L47. When the TCP request reaches the network interface card, an outer IP header is added so as to route the request to the router 26 in Figure 1. The outer IP header is a virtual tunnel header which has a locally unique source IP address of 10.0.0.1 (the local IP address of the network device) and a locally unique destination IP address of 10.0.0.7 which the the local IP address of the router 26. The inner IP header has the true globally unique IP addresses of the LAN and the server on the internet to which the TCP packet is directed. The network interface card basically encapsulates the inner IP header and its packet with an outer IP header and sends the encapsulated packet to the router. C15/L47-67, see Table 3. The outer IP header is stripped when the encapsulated packet reaches the router 26, and the packet with the inner IP header is then sent out on the internet. If the inner packet were an IPsec packet, and in encountered any NAT or protocol conversions on its path to the destination device, the IPsec packet would be rendered unusuable by the NAT or protocol conversion.

Inbound packets have the same process carried out at the router. Specifically, an outer IP header with the locally unique IP addresses of 10.0.0.7 for the router and 10.0.0.1 for the network device which made the original request are added to the packet. As was the case for the outbound packets, the locally unique IP addresses are not globally unique and must be stripped off before the packet is sent out onto the internet.

The encapsulation taught in Nessett is not the same encapsulation recited in the claims at bar. DNAT as taught in Nessett is essentially a process of making a combination network address by appending an outer IP header to a packet with an inner IP header which has unique globally addressable IP addresses. The outer IP header has only locally unique IP addresses. Thus, the encapsulation of Nessett taught at Col 15 et seq. is not the encapsulation taught in the invention because the outer IP headers get stripped off before the packet is sent on the internet. This would not work in the method of the invention as it is the outer headers which are added which fool the NATs into thinking the inner IPsec packets (or whatever other protocol packets which cannot traverse NAT without damage) are UDP or TCP packets or other protocol packets which can traverse NAT without damage. These outer headers in the invention must stay on the packets till while they traverse the internet and until they reach their destination nodes (the destination end of the tunnel in the case of VPN tunneling using IPsec) where they can be stripped off.

No different encapsulation is taught at Col. 26, line 8 through Col. 28, line 34 where DNAT with security is taught. In that method of Nessett, the same encapsulation for transmissions between the LAN network device and the router is used and the PAP protocol is used not only to obtain the locally unique port numbers but also the locally unique SPI values. Thus, this encapsulation is different than in the claims at bar.

PATENT

Respectfully submitted,

Dated: July 22. 2003

Ronald Craig Fish
Reg. No. 28,843
Tel 408 778 3624
FAX 408 776 0426

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail, postage prepaid, in an envelope addressed to: Commissioner for Patents , P.O. Box 1450, Alexandria, Va. 22313-1450.

on July 22, 2003
(Date of Deposit)

Ronald Craig Fish, President
Ronald Craig Fish, a Law Corporation
Reg. No. 28,843